DPRIVE FAQ

Updated 4/22/2020

Q1: Does DARPA anticipate DPRIVE awards to be ITAR controlled?

A1: ITAR controls are not anticipated. Performers are responsible for making ITAR determinations for their respective proposals, working with their export compliance office and/or Departments of Commerce and State.

Q2: How will test and evaluation (T&E) be performed on deliverables?

A2: T&E will be based on the metrics provided in the BAA. T&E specifics will be determined once the DARPA selected T&E government team has been assembled.

Q3: How should proposals address attack vectors or assumed information about adversary attacks/intent?

A3: The DPRIVE program is not addressing cryptanalysis.

Q4: Will the hardware board hosting the final chip be GFE or otherwise standardized across the program?

A4: No. Proposers must supply all supporting hardware, including mother boards, software, instrumentation, etc. to support operation of the DPRIVE coprocessor. Such hardware and software should be included in the cost proposal. It is not anticipated that this will be a significant driver on cost or performance.

Q5: Will DARPA provide an anticipated breakdown of performance improvements across the accelerator architecture (HW, SW, Algorithms)?

A5: It is up to the proposers to provide this information as derived from their approach.

Q6: Are FPGA or GPU solutions acceptable?

A6: No, the use of FPGA and GPU solutions is not consistent with the goals of the program. A unique accelerator implementation addressing FHE computation is desired.

Q7: Are all design files expected as government purpose rights (GPR) and required as deliverables? What if the coprocessor design includes 3rd party IP libraries and blocks that cannot be provided as GPR?

A7: It is anticipated that all hardware, software, and algorithm developments that are funded by an award under DPRIVE will be delivered to the US Government and have unlimited rights. 3rd party IP that was not developed under a DPRIVE award is not considered a deliverable or to have unlimited rights.

Q8: What foundry and fabrication process will be provided for the GFE/GFI shuttle runs?

A8: DARPA MTO shuttle runs will use the GF 12 nm 21B 14LP process.

Q9: Is hardware support for Bootstrapping within scope of DPRIVE?

A9: Yes.

Q10: Can proposals assume some quantization of the neural networks or must the accelerator compute on floating point data?

A10: Fixed-point implementation under FHE algorithms to assume single precision floating point accuracy is expected. DPRIVE is not concerned with optimizing neural network operations or advancing the state of the art in neural networks.

Q11: How should proposers interface with users/programmers? Do proposers need to build compilers in order to map software libraries to hardware accelerator components?

A11: The approach of software programmability of the DPRIVE coprocessor is the responsibility of the proposer. Software control of the DPRIVE coprocessor is expected to achieve the program goals. Proposers are guided to the IARPA HECTOR program as an example of existing efforts in this area. Proposers must provide the ability to access and utilize the DPRIVE accelerator within the software of the integrated host CPU system. The ability for users/programmers to utilize the DPRIVE accelerator within the software coding of the host CPU system must be supported.

Q12: What is meant by formal verification?

A12: As per the language in Sections I.B and I.F of the BAA, formal verification assures that a circuit design represents a circuit that does what it is intended to do and nothing more. The formal verification will not only validate the circuit design for accuracy, but will also provide a scalable and automatable proof of correctness that the circuit performance is formally verifiable under all circumstances.

Q13: What security level is required under DPRIVE?

A13: A security parameter (lambda) value of 128 is required (for a description of this parameter, see Acar *et. al.*, *A Survey on Homomorphic Encryption Schemes: Theory and Implementation, Sections 3 and 4).*

Q14: What is the award size?

A14: DPRIVE is anticipating a total budget of $33M over a 42 month period of performance, across all selected performers.

Q15: What is the schedule for chip tape out and will performance be on hold during the tape-out window?

A15: Final tape out and device fabrication is expected to happen immediately after the Phase 3 option award, and last for a duration of ~3 months. Performer activities will continue during this window, with a focus on software and test HW development.

Q16: Does DARPA expect a specific FHE library to be utilized?

A16: The choice of FHE library and implementation is up to the proposer.

Q17: Should proposers draw from the PROCEED program?

A17: This is not required.

Q18: Is DPRIVE targeting cloud or edge/embedded accelerator implementations?

A18: The system implementation is not a specific goal of the program. Proposals should provide a viable implementation and transition approach for a single chip solution that is scalable from embedded to cloud applications.

Q19: Are classical security approaches acceptable to DPRIVE?

A19: No. Lattice based approaches have been proven quantum secure. DPRIVE will only accept lattice based FHE schemes.

Q20: Can proposals provide partial solutions such as only hardware or only software?

A20: No, proposals must address a complete solution to include hardware, software, and algorithms. This is why teaming is strongly encouraged, where the team members bring together their expertise in hardware, software, and algorithms to arrive at their version of a full DPRIVE solution.

Q21: Does the requirement of a 10^5 speed up in FHE computation time need to be demonstrated in phase 1 (15 months)?

A21: As per Section I.C and Figure 5 of the DPRIVE BAA, Phase 1 is focused on designing the core FHE ALU building blocks. Emulated performance of these building blocks should demonstrate the path to achieving the FHE computational speeds that meet the BAA's metrics.

Q22: Will DARPA accept FHE schemes other than BGV (i.e. FHHE, BFV, etc.)?

A22: All proposed solutions must be able to run the BGV FHE scheme in order to provide a means of comparing computation times across performers. The core arithmetic and logic blocks are common between various FHE schemes. Proposals that support multiple FHE schemes are acceptable as described in Section F of the BAA. An amendment to the BAA will be published soon which will specify that, at a minimum, BGV must be supported to enable a comparison.

Q23: Is DARPA interested in approximate arithmetic vs exact arithmetic?

A23: The BAA describes computations for logistic regression and CNN training and inference without allowances for approximate arithmetic and therefore exact mathematics is expected.

Q24: Does DPRIVE require solutions that use large arithmetic word size for large bit multipliers?

A24: No. If there are solutions that meet the run-time goals of the program without the need for computing on large bit word sizes, this would be acceptable. Based on studies to date, LAWS-based approaches are of specific interest.

Q25: Does DPRIVE have any power requirements for the accelerator?

A25: No, DPRIVE has no specific power requirement but it will be a consideration.

Q26: Is DARPA interested in architectures that can support SIMD?

A26: DPRIVE is looking for architectures that optimize FHE computation. The consideration of SIMD for the implementation of FHE computation is up to the proposer.

Q27: If two multiplication schemes are better for different mathematics, how should a choice between the two be made?

A27: Multiple multiplication schemes are not required. Implementation choices should be made based on meeting the metrics in the BAA as far as speed, size, and parameters.

Q28: Will DARPA accept proposals that provide non-levelled FHE solutions?

A28: Levelled and non-levelled approaches will be considered.

Q29: Why is DPRIVE focused on a 7 layer CNN?

A29: We have selected a popular CNN configuration that is well explored by the community. Running this CNN in a homomorphic manner should impose considerable challenge. Remember, the DPRIVE program is not focused on advancing the state of the art in neural networks, thus an established neural net design is called for here.

Q30: Will I/O requirements or other IP for the accelerator design be provided by the government?

A30: No. IP or functional design implementations for the accelerator will NOT be provided by the government.

Q31: Will the government or the performer be assuming the costs of packaging of the DPRIVE device?

A31: The performer is responsible for the cost of packaging and mounting the DPRIVE accelerator. Such costs should be included in the cost proposal.

Q32: Is there a side-channel leakage security requirement?

A32: Side-channel leakage and attack security are not part of the DPRIVE program.

Q33: Will the government be providing performers access to ASIC emulation / verification platforms such as Cadence's Palladium or Synopsys's ZeBu?

A33: DARPA is working with the Air Force Research Lab (AFRL) for access and use of their Palladium tools and installation for use by DPRIVE performers. An amendment to the BAA will be published soon which will describe this as Government Furnished Facilities and seek from proposer information regarding their expected access requirements. Use of the AFRL Palladium system is not required.

Q34: Does the DPRIVE chip also need to implement both encryption and decryption of the data, or only the specified mathematical operations on already encrypted data?

A34: The DPRIVE chip needs to implement the specified mathematical operations on already encrypted data, the chip does not need to implement encryption and decryption operations.

Q35: Does the GF Shuttle process include packaging, or does it return only bare die?

A35: The GF Shuttle process will return a bare die, the process does not include packaging. Please also refer to Q and A #31.

Q36: The cover sheets for the abstract, technical, and cost volume request the proposer to identify a "Technical Area" - however, it is my understanding based on pages 13-14 of the BAA that "DPRIVE will have a single Technical Area." Can you advise on what would be an acceptable input in the "Technical Area" section of the cover sheets? Would "N/A" be acceptable or should we indicate "one" or "all" or something else?

A36: When filling out the cover sheet topic “Technical area(s)”, since there is a single technical area for the DPRIVE program, please simply respond “Technical area(s): DPRIVE.”

Q37: Regarding industrial collaborator, is it allowed to team with a US company but the specific team is out of US? Or it has to be inside US?

A37: Foreign participants/resources may participate to the extent allowed by applicable Security Regulations, Export Control Laws, Non-Disclosure Agreements, and appropriate regulations. These include: FAR/DFARS Part 27.7 "Prohibited Sources"; BAA IV “Application and Submission Information”, B “Content and From of Application Submission,” 2. “Full Proposal Format”, II “Detailed Proposal Information”, Item H "National Security Impact Statement," particularly Paragraph 4 and 4. “Security Information”; and BAA V “Application Review Information”, A "Evaluation Criterion”, 2 "Potential Contribution and Relevance to the DARPA Mission and Technology Transition", which relate to the topic of foreign participation and/or transition to foreign entities.

Q38: Where are the slides from the Proposers day available online?

A38: The DPRIVE Proposers Day video is posted at https://www.darpa.mil/work-with-us/opportunities

The DPRIVE Proposers Day presentations are posted for download at the same site.

Q39: Does the government anticipate that any CUI will be developed during this effort?

A39: It is anticipated that it is quite possible that there will be controlled unclassified information (CUI) developed on the DPRIVE program. A DPRIVE CUI guide will be provided for proposals selected for the DPRIVE program.

Updated 4/22/2020

Q40: Are all the mathematical operations assumed to be ciphertext-ciphertext? I.e. do both the model weights and inputs for the example machine learning applications need to be encrypted or are the model weights assumed to be plaintext?

A40: All mathematical operations will be ciphertext-ciphertext. All data inputs, including model weights, will be encrypted.

Q41: For the technical point of contact listed on the proposal cover sheets, if there are two individuals sharing the PI lead of the proposed effort, how should the two individuals sharing the role of lead PI be listed?

A41: There needs to be a single PI identified for a proposed effort. There can be Co-PIs, but there must be one, sole lead PI for the proposed effort that is listed on the proposal cover sheet.

Q42: What is the reasoning that leads to the statements in the last paragraph of page 8 of the DPRIVE BAA, "Word size directly relates to the signal-to-noise ratio (SNR)... large arithmetic word size (LAWS) increases SNR in the FHE computations..", and the curve in Figure 2 on page 9 of the BAA, and is the report from which those results were derived available for review?

A42: The SNR is related to random noise imposed on the lattice arithmetic, as well as accumulated round off errors. Larger word sizes make the accumulated noise and errors have less impact on the word accuracy. Figure 2 on p. 9 of the DPRIVE BAA was produced by Palisades runs to get order of magnitude estimates of computational time as a function of word size.

Q43: For the neural network topology specs in the DPRIVE BAA, is there is a mismatch between layers 12 and 13. The number of neurons at the output of layer 12 is 4096 but layer 13 expects 1024 input nodes. Is this understanding correct? If this is the case, would there be an extra average pooling layer between layer 12 and 13 to make the numbers match?

A43: Please refer to the cited reference for this design, which we repeat as follows: Figure 13 of Jian Liu, Mika Juuti, Yao Lu, and N. Asokan. “Oblivious neural network predictions via minionn transformations,” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017, pages 619–631, 2017.

Q44: Due to COVID-19 impacts, will the DPRIVE BAA proposal due date of June 2 be extended?

A44: Currently, there are no plans to modify or extend the DPRIVE BAA proposal due date. DARPA is monitoring the situation. If the DPRIVE BAA due date is changed, it would be effected as an amendment published on beta.SAM.gov (which should be monitored on a regular basis).